# Employee Post-Travel Disclosure of Travel Expenses

Date/Time Stamp:

Post-Travel Filing Instructions: Complete this form within 30 days of returning from CRETARY OF THE SENATE travel. Submit all forms to the Office of Public Records in 232 Hart Building. 17 SEP 20 PM 4: 27 In compliance with Rule 35.2(a) and (c), I make the following disclosures with respect to travel expenses that have been or will be reimbursed/paid for me. I also certify that I have attached: ☑ The original Employee Pre-Travel Authorization (Form RE-1), AND A copy of the Private Sponsor Travel Certification Form with all attachments (itinerary, invitee list, etc.) Private Sponsor(s) (list all): Stanford University's Hoover Institution 08/14/2017 - 08/17/2-17 Travel date(s): Name of accompanying family member (if any): N/A Relationship to Traveler: 

Spouse ☐ Child IF THE COST OF LODGING DID NOT INCREASE DUE TO THE ACCOMPANYING SPOUSE OR DEPENDENT CHILD, ONLY INCLUDE LODGING COSTS IN EMPLOYEE EXPENSES. (Attach additional pages if necessary.) Expenses for Employee: Other Expenses Meal Expenses **Lodging Expenses** Transportation (Amount & Description) Expenses ☐ Good Faith \$82.63 - Ground Transportation \$182.50 \$450 Estimate \$0 - Flight Actual Amount Expenses for Accompanying Spouse or Dependent Child (if applicable): Other Expenses Meal Expenses **Lodging Expenses** Transportation (Amount & Description) Expenses ☐ Good Faith N/A N/A N/A Estimate N/A ☐ Actual Amount Provide a description of all meetings and events attended. See Senate Rule 35.2(c)(6). (Attach additional pages if necessary.): Ç)

See Attached Syllabus

**D**DDDD

0000

19/2017 Nicholæs A. Rossi (Printed name of traveler)

(Signature of traveler)

TO BE COMPLETED BY SUPERVISING MEMBER/OFFICER:

I have made a determination that the expenses set out above in connections with travel described in the Employee Pre-Travel Authorization form, are necessary transportation, lodging, and related expenses as defined in Rule 35.

(Signature of Supervising Senator/Officer)

# PRIVATE SPONSOR TRAVEL CERTIFICATION FORM

This form must be completed by any private entity offering to provide travel or reimbursement for travel to Senate Members, officers, or employees (Senate Rule 35, clause 2). Each sponsor of a fact-finding trip must sign the completed form. The trip sponsor(s) must provide a copy of the completed form to each invited Senate traveler, who will then forward it to the Ethics Committee with any other required materials. The trip sponsor(s) should NOT submit the form directly to the Ethics Committee. Please consult the accompanying instructions for more detailed definitions and other key information.

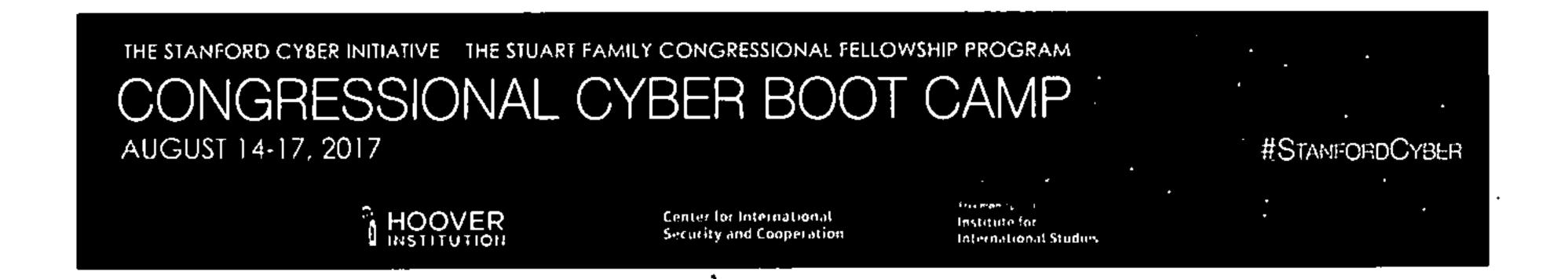
The Senate Member, officer, or employee MUST also provide a copy of this form, along with the appropriate travel authorization and reimbursement form, to the Office of Public Records (OPR), Room 232 of the Hart Building, within thirty (30) days after the travel is completed.

Desc	ription of the trip: An intensive program for congressional staff which consists of three days of
	inars, simulations, and keynote presentations.
Date	s of travel:
	e of travel: Stanford University, Palo Alto, CA
	e and title of Senate invitees: See attached list
l cer	tify that the trip fits one of the following categories:
1	(A) The sponsor(s) are not registered lobbyists or agents of a foreign principal and do not retain or employ registered lobbyists or agents of a foreign principal and no lobbyist or agents of a foreign principal will accompany the Member, officer, or employee at any point throughout the trip.  - OR -
1	(B) The sponsor or sponsors are not registered lobbyists or agents of a foreign principal, but retain or employ one or more registered lobbyists or agents of a foreign principal and the trip meets the requirements of Senate Rule 35.2(a)(2)(A)(i) or (ii) (see question 9).
	I certify that the trip will not be financed in any part by a registered lobbyist or agent of a foreign principal.  - AND -
	I certify that the sponsor or sponsors will not accept funds or in-kind contributions earmarked directly or indirectly for the purpose of financing this specific trip from a registered lobbyist or agent of a foreign principal or from a private entity that retains or employs one or more registered lobbyists or agents of a foreign principal.
X	rtify that:  The trip will not in any part be planned, organized, requested, or arranged by a registered lobbyist or agent of a foreign principal except for de minimis lobbyist involvement.  - AND -
X	The traveler will not be accompanied on the trip by a registered lobbyist or agent of a foreign principal except as provided for by Committee regulations relating to lobbyist accompaniment (see question 9).

9.	USE ONLY IF YOU CHECKED QUESTION 6(B)  I certify that if the sponsor or sponsors retain or employ one or more registered lobbyists or agents of a foreign principal, one of the following scenarios applies:
	<ul> <li>□ (A) The trip is for attendance or participation in a one-day event (exclusive of travel time and one overnight stay) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee on any segment of the trip.</li> <li>+ OR -</li> </ul>
	<ul> <li>□ (B) The trip is for attendance or participation in a one-day event (exclusive of travel time and two overnight stays) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee on any segment of the trip (see questions 6 and 10).</li> <li>- OR -</li> </ul>
	(C) The trip is being sponsored only by an organization or organizations designated under § 501(c)(3) of the Internal Revenue Code of 1986 and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee at any point throughout the trip.
10.	USE ONLY IF YOU CHECKED QUESTION 9(B)  If the trip includes two overnight stays, please explain why the second night is practically required for Senate invitees to participate in the travel:
11.	An itinerary for the trip is attached to this form. I certify that the attached itinerary is a detailed (hourby-hour), complete, and final itinerary for the trip.
12.	Briefly describe the role of each sponsor in organizing and conducting the trip:
	Stanford University's Hoover Institution solely planned all aspects of the trip, including topics to be
	discussed, travel/accommodation logistics, and required paperwork. Hoover employees will also be
	responsible for traveling with congressional staff and managing logistics for the duration of the trip.
13.	Briefly describe the stated mission of each sponsor and how the purpose of the trip relates to that mission:
	The Hoover Institution is a research institution that seeks to improve the human condition by advancing
	ideas that promote economic opportunity and prosperity while securing and safeguarding the peace
	through its world renowned scholars, library, and archives, as well as by engaging Congress and its staff.
14.	Briefly describe each sponsor's prior history of sponsoring congressional trips:
	This is the third sponsored trip for congressional staff organized by the Hoover
	Institution. The latest of which was in April of 2017 and had a similar format as this trip.

Stanford University's Hoover Institution regularly sponsors policy panels and roundtables for think tank scholars, journalists, congressional staff, Executive branch officials, academics, and members of the						
Total Expenses for Each Participant:						
	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expense		
⊠ Good Faith estimate	\$0 roundtrip airfare; \$200 ground transportation	\$450 total (\$150/night)	\$192 total (\$64/day)	N/A		
Actual Amounts						
· · · · · · · · · · · · · · · · · · ·	rip involves an event the trip involves an event oation:	<del>-</del>	_			
participation or b) the congressional particip	e trip involves an event	that is arranged or org	ganized specifically v			
participation or b) the congressional participation.  The trip is arranged/c	e trip involves an event pation:	that is arranged or org	ganized specifically v			
participation or b) the congressional participation. The trip is arranged/c.  Reason for selecting to the congressional participation.	e trip involves an event pation: organized specifically for	that is arranged or org	ganized specifically v	vith regard to		
Participation or b) the congressional participation. The trip is arranged/c.  Reason for selecting to the congressional participation.	e trip involves an event pation: organized specifically for the location of the event	that is arranged or org	ipation. ticipate in the event,	vith regard to		
Participation or b) the congressional participation. The trip is arranged/c.  Reason for selecting to the Hoover Institution.	e trip involves an event pation: organized specifically for the location of the event phificant number of Hoo	that is arranged or orgonal partice or trip ver senior fellows partices and the stanford University can	ipation. ticipate in the event,	vith regard to		
Participation or b) the congressional participation. The trip is arranged/or Reason for selecting to the Hoover Institution. Name and location of	e trip involves an event pation: organized specifically for the location of the event phificant number of Hoods has beadquarters on the	that is arranged or orgonal partice or trip ver senior fellows partices Stanford University can facility:	ipation. ticipate in the event,	vith regard to		
Participation or b) the congressional participation. The trip is arranged/or Reason for selecting to the Hoover Institution. Name and location of Schwab Residential of the Schwab Residential of the Hoover Institution.	the location of the event inficant number of Hoo h's headquarters on the	that is arranged or orgonomy congressional partice or trip ver senior fellows partices Stanford University can facility: Stanford, CA 94305	ipation. ticipate in the event,	vith regard to		

	Describe how the daily expenses for lodging, meals, and other expenses provided to trip participants compares to the maximum per diem rates for official Federal Government travel:				
Α	Il lodging, meals, and other expenses are within the official federal government travel per diem rate for				
P:	alo Alto, CA.				
cla	escribe the type and class of transportation being provided. Indicate whether coach, business-class or first ass transportation will be provided. If first-class fare is being provided, please explain why first-class avel is necessary:				
s	tanford University's Hoover Institution will provide round-trip ground transportation between SFO airport				
a	ind Stanford University.				
2	I represent that the travel expenses that will be paid for or reimbursed to Senate invitees do not include expenditures for recreational activities, alcohol, or entertainment (other than entertainment provided to all attendees as an integral part of the event, as permissible under Senate Rule 35).				
th	st any entertainment that will be provided to, paid for, or reimbursed to Senate invitees and explain why e entertainment is an integral part of the event:  one				
co Si	nereby <i>certify</i> that the information contained herein is true, complete and correct. (You must include the impleted signature block below for each trayel sponsor.):  gnature of Travel Sponsor:				
Na	ame and Title: Michael G. Franc, Director of Washington, DC Programs				
Na	ame of Organization: Hoover Institution				
A	dress: 1399 New York Ave NW, Suite 500, Washington, DC 20005				
	lephone Number: (202) 760-3200				
	x Number: (202) 760-3191				
	mail Address:mfranc@stanford.edu				



# SYLLABUS

# **FACULTY CO-CHAIRS**

# Dr. Amy Zegart

Co-Director, Center for International Security and Cooperation (CISAC) Davies Family Senior Fellow, Hoover Institution Senior Fellow, Freeman Spogli Institute for International Studies (FSI) Professor of Political Science (by courtesy), Stanford University

## Dr. Herb Lin

Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)

Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National
Academies

# **COURSE DESCRIPTION**

Modern nations are increasingly dependent on information and information technology for societal functions. Thus, ensuring the security of information and information technology — cybersecurity — against a broad spectrum of hackers, criminals, terrorists, and state actors is a critical task for the nation. Cybersecurity challenges are evolving at a rapid pace, and the cyber threat the nation faces today will be different from the one it faces tomorrow.

Cybersecurity is not solely a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, and a host of other disciplines. Therefore, this Boot Camp draws upon the expertise of cyber scholars in academia as well as senior business and security professionals in Silicon Valley to provide perspectives on the many dimensions of this dynamic issue.

This Boot Camp will integrate multiple perspectives and disciplines to provide an understanding of the fundamentals of cybersecurity, the nature of cybersecurity threats, various approaches to

addressing these threats, and the use of offensive cyber capabilities to advance national interests. The Stanford Cyber Boot Camp endeavors to give congressional staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the problems of tomorrow.

# Day 1 (Monday, August 14): Cyber Attacks and Responses

12:00 p.m. - 1:00 p.m.: Lunch & Keynote Address

# **RE-FRAMING THE "CYBERSECURITY" PROBLEM**

# Faculty:

- Sean Kanuck, Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence; CISAC affiliate
- Introduction: Dr. Herb Lin, Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution

This session will overview the scope of the program (what we cover, what we don't, and why) and set the analytic stage for how we approach the rest of the course.

- Scope: The security implications and challenges of the nation's use of information technology. The course does not address topics such as consumer security, although many concepts covered are relevant.
- Framing Theme #1: Cybersecurity has different meanings and poses different challenges
  to different stakeholders. Approaching the problem posed requires understanding the
  perspectives of various actors, their interests, incentives, and organizational demands.
  Boot Camp sessions are designed to allow staffers to better understand the perspectives
  of different stakeholders and key players, including attackers and corporate executives.
- Framing Theme #2: The non-technical dimensions of cybersecurity (politics, organizational dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.
- Framing Theme #3: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.
- Framing Theme #4: The Boot Camp explains the inherent dominance of offense over defense in cybersecurity and how this fact relates to the "cybersecurity problem."

1:00 p.m. - 2:00 p.m.: Session 1

### THINKING LIKE AN ATTACKER

# Faculty:

- Dr. Earl Boebert, Senior Scientist, Sandia National Laboratories (Retired)
- Dr. Herb Lin, Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

<u>Assignment:</u> While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

<u>Learning Objectives:</u> Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

2:30 p.m. - 3:30 p.m.: Session 2

# THREATS TO CYBERSECURITY

### Faculty:

 Carey Nachenberg, Google X; Adjunct Assistant Professor of Computer Science, UCLA

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. Session 2 examines these compromises and the vulnerabilities in information technology that allow them to happen, again reprising the theme of offensive dominance. This session will include a number of forensic case studies that illuminate the attack spectrum, key challenges, and trends.

<u>Learning Objectives</u>: Security-relevant principles of information technology; types of compromise; the inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

# 3:45 p.m. – 4:15 p.m.: Keynote Remarks

## THE VIEW FROM EUROPE

# **Faculty:**

- Toomas Hendrik Ilves, Former President of Estonia; Distinguished Visiting Fellow at CISAC, Hoover, and FSI
- Introduction: Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

4:30 p.m. - 5:30 p.m.: Dinner & Session 3

## OFFENSIVE DIMENSIONS OF CYBERSECURITY

# **Faculty:**

- Jason Healey, Senior Research Scholar, Columbia University's School for International and Public Affairs; Hoover Visiting Fellow; CISAC Affiliate
- Dr. Herb Lin (Discussant), Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution

Offensive activities — including those conducted for espionage and attack purposes —serve a variety of national goals. These goals include, but are not limited to, cyber defense. This discussion will summarize the required strategy, intelligence, and policy necessary for offensive cybersecurity.

<u>Learning Objectives</u>: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture and for other purposes; the differences between attacks and exploitations and the importance of these differences; the scope and nature of U.S. command and control of offensive operations in cyberspace.

6:00 p.m. - 8:30 p.m.: Session 4

# SIMULATION: RESPONDING TO A CYBER CRISIS

# **Faculty:**

- Michael McNerney, Co-Founder and CEO of Efflux Systems; CISAC Affiliate
- Raj Shah, Managing Partner, Defense Innovation Unit Experimental (DIUx)
- Joe Sullivan, Chief Security Officer, Uber
- Ruby Zefo, Vice President of the Law & Policy Group and Chief Privacy & Security Counsel, Intel Corporation
- Dr. Amy Zegart (Chair), Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

In this exercise, congressional staffers assume the roles of business executives at a large tech company called Frizzle that has just discovered a major cyber breach. Early forensics indicate that a Frizzle employee opened a malicious PDF file containing a zero-day exploit. This vulnerability enabled the attackers to gain access to F-Net, the company's social networking platform, as well as the Frizzle email user accounts of Chechen activists and sympathizers. In addition, the malicious file may have spread through victims' emails to the Credit Luxe bank in Luxembourg, which processes more than two thirds of Frizzle's user payments. Frizzle's engineering/cybersecurity team, which is one of the best in the world, believes the attack came from Eastern Europe, though much remains unclear.

The CEO has called an emergency meeting of the Board of Directors to formulate a broad-based response to the cyber breach and has asked each of Frizzle's core teams – Engineering / Cybersecurity, Business Strategy, Legal, Public Policy, and Marketing / Communications – to develop and present actionable recommendations to the Board.

The Board of Directors is played by leading Silicon Valley security specialists, lawyers, and entrepreneurs with extensive experience in cybersecurity and business. Board Members attend team breakout sessions and in the "full board meeting" question and discuss each team's recommendations. The simulation concludes with a debrief session where staffers reflect on the simulation and Board Members share insights from their actual experiences confronting cyber challenges.

<u>Learning Objectives</u>: To walk in the shoes of business leaders confronting the early hours and critical decisions of a cyber crisis. Who exactly is hurt or could be hurt by the breach? How could the breach impact Frizzle's business in different markets and its brand reputation? Who are the

key stakeholders and how might they react? What actions should Frizzle take and what are the tradeoffs? Should the company "hack back" or publicize the breach to its users, its European bank, its competitors? Work with U.S. government agencies? How do Frizzle's mission and corporate culture guide its response? These are some of the questions staffers will consider.

# Day 2 (Tuesday, August 15): Deep Dive: Technical & Nontechnical Aspects of Cyber

8:30 a.m. – 10:00 a.m.: Breakfast and Keynote Conversation

**KEYNOTE** 

Industry and Policy Challenges in Cybersecurity

# **Faculty:**

- **Dr. Condoleezza Rice,** Thomas and Barbara Stephenson Senior Fellow, Hoover Institution; Denning Professor, Stanford Graduate School of Business; former U.S. Secretary of State and National Security Advisor
- Marc Andreessen, Co-Founder and General Partner of Andreessen Horowitz
- Introduction: Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

10:15 a.m. - 11:15 a.m.: Session 5

# **FUNDAMENTAL PRINCIPLES OF CYBERSECURITY**

# **Faculty:**

- Dr. Irving Lachow, Portfolio Manager, International Cyber, MITRE; Visiting Fellow, Hoover Institution; Affiliate, CISAC
- Dr. John Villasenor, Professor of Electrical Engineering, Public Policy, and Management, UCLA; Visiting Professor of Law, UCLA; Visiting Fellow, Hoover Institution; Affiliate, CISAC

Although cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the fundamental principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

<u>Learning Objectives</u>: The value of these fundamental principles of cybersecurity and how they can be used collectively to improve security.

11:45 a.m. - 12:45 p.m.: Lunch & Session 6

# **ECONOMIC & ORGANIZATIONAL DIMENSIONS OF CYBERSECURITY**

# Faculty:

- Dr. Dave Clark, Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory
- Dr. Tyler Moore, Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa

Known cybersecurity measures are often fully adopted due to a variety of economic and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. An organizational perspective addresses the structural necessities and importance of organizational culture to cybersecurity. This session examines how these factors often discourage the adoption of sound security practices.

<u>Learning Objectives</u>: The importance of economic and organizational factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

1:30 p.m. - 2:30 p.m.: Session 7

# DOMESTIC LAW AND INTERNATIONAL LEGAL DIMENSIONS OF CYBER SECURITY

# Faculty:

- Prof. Matthew Waxman, Liviu Librescu Professor of Law, Faculty Chair Roger Hertog Program on Law and National Security, Columbia University
- Prof. Robert Chesney, Associate Dean and Charles I. Francis Professor, University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law

Technological change has far outpaced changes in law and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technology. Furthermore, nations have cooperative and competitive (and sometimes adversarial) interests that play out in cyberspace. Internet communication does not inherently respect national borders, giving an international dimension to every cybersecurity challenge.

<u>Learning Objectives</u>: For domestic law, the implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing law to technological circumstances not contemplated at the time of initial passage.

For international dimensions, various legal regimes of potential relevance, including the law of war, human rights law, trade and intellectual property law; proposals for Internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

2:30 p.m. – 3:00 p.m.

# **DEBRIEF from previous day**

# Faculty:

- Dr. Herb Lin, Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution
- Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

3:00 p.m. – 4:00 p.m.

### **HOOVER ARCHIVES OR STANFORD WALKING TOUR**

- Archive Tour: Jean Cannon, Assistant Archivist Communications & Outreach
- Walking tour: Rachel Hirshman, Stanford Student

5:30 p.m. – 8:30 p.m.: Reception & Dinner

KEYNOTE

Cyber Challenges From the C-Suite to the Kremlin

### Faculty:

- Dr. Michael McFaul, Director and Senior Fellow, FSI; Peter and Helen Bing Senior Fellow, Hoover Institution, Professor of Political Science, Stanford University; former U.S. Ambassador to the Russian Federation
- Joel Peterson, Chairman, JetBlue Airways; Robert L. Joss Adjunct Professor of Management, Stanford Graduate School of Business; Chairman, Hoover Institution Board of Overseers
- Introduction: Mike Franc, Director, Hoover DC office

 Moderator: Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

# Day 3 (Wednesday, August 16): Civil Liberties, Corporate Interests, and Security

7:45 a.m. - 8:30 a.m.: Breakfast

# **DEBRIEF** from previous day

# Faculty:

- Dr. Herb Lin, Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution
- Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

### 8:30 a.m. - 9:30 a.m.: Session 8

# **CYBERSECURITY AND CIVIL LIBERTIES**

# **Faculty:**

- Anne Neuberger, Deputy Director of Operations, National Security Agency
- Jennifer Granick, Director of Civil Liberties, Stanford Center for Internet and Society; Affiliate, CISAC; Former Civil Liberties Director, Electronic Frontier Foundation

Measures intended to support cybersecurity can also threaten certain civil liberties. What cybersecurity means depends in part on whose security is at risk. For some, a threat to civil liberties resulting from greater use of information technology might be interpreted as a cybersecurity threat. Session 8 focuses on this push and pull between security and civil liberties in cyberspace.

<u>Learning Objectives</u>: Different perspectives at the nexus of civil liberties and cybersecurity; how, when, and to what extent, preservation of civil liberties and cybersecurity trade off against one another. Topics to be discussed include privacy, anonymity, and free speech.

9:30 a.m. - 10:30 a.m.: Session 9

# **INDUSTRY PERSPECTIVES ON CYBERSECURITY**

# Faculty:

- Dr. Sameer Bhalotra (Chair), Co-Founder and CEO, StackRox; Senior Associate
  of the Strategic Technologies Program, CSIS; Affiliate, CISAC; former Senior
  Director for Cybersecurity, National Security Council
- Bandel Carano, Managing Partner, Oak Investment Partners
- Rick Howard, Chief Security Officer, Palo Alto Networks
- Claire Hughes Johnson, COO, Stripe
- Matt Miller, Partner, Sequoia Capital

Market forces have a critical role in enhancing or weakening cybersecurity. Session 9 examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "cyberground truths" about the security problems facing the private sector.

<u>Learning Objectives</u>: Various private sector perspectives from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity.

11:00 p.m. - 11:45 p.m.: Session 10

WHITE HOUSE PERSPECTIVES

# **Faculty:**

Andy Grotto, CISAC Perry Fellow; Hoover Research Fellow; Affiliate, CISAC;
 Former Senior Director for Cybersecurity Policy, National Security Council

12:00 p.m. – 1:30 p.m.: Lunch Keynote

DRIVERLESS CARS & PLANE HACKING: SECURITY VULNERABLITIES, CAUSES, AND CHALLENGES

### Faculty:

Dr. Stefan Savage, Professor of Computer Science and Engineering, UCSD;
 Director, Center for Network Systems (CNS); Co-Director, Center for Evidence-based Security Research (CESR)

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced a range of new potential risks. In 2010, University of California, San Diego and the University of Washington demonstrated the ability to remotely control a popular passenger vehicle with no prior physical access. Recent demonstrations have validated that similar issues exist in other vehicles as well.

<u>Learning Objectives</u>: The nature of automotive security vulnerabilities, the underlying causes, and the challenges (both technical and non-technical) in securing the automotive platform.

2:30 p.m. - 4:30 p.m.

# **TESLA FACTORY VISIT**

Technology companies are leading innovation and changing the world. Tesla was founded in Silicon Valley in 2003 with the goal to manufacture zero-emission electric cars and has experienced goal exponential growth in this field. Today Tesla has expanded its mission to specialize in batteries and sustainable solar energy. While this transformation has driven major advancements in efficiency, it has also introduced a range of new potential cyber risks.

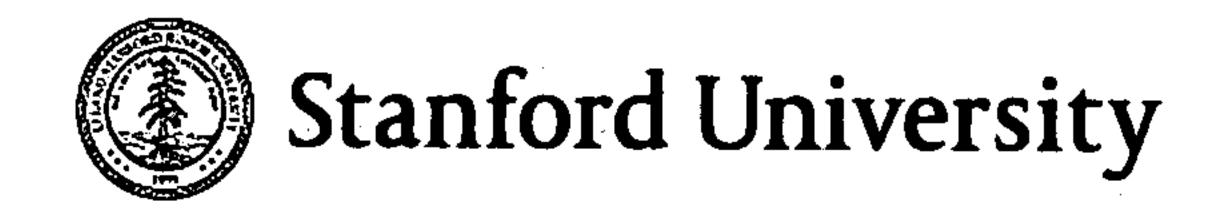
<u>Learning Objectives</u>: By engaging directly with senior engineers at the Tesla Factory, Congressional staffers will be exposed to the complexities of a tech firm at the center of innovation.

Tesla Factory 45500 Fremont Blvd, Fremont, CA 94538

6:30 p.m. – 8:30 p.m.

**DINNER: Debrief & Next Steps** 

Coupa Café – Stanford Golf Course 198 Junipero Serra Blvd, Stanford, CA, 94305



Dear Mr. Rossi,

On behalf of Hoover Institution fellows Mike Franc, Herb Lin and Amy Zegart, I would like to formally invite you to participate in Stanford's Congressional Cyber Boot Camp, held in Palo Alto, California on August 14<sup>th</sup> – 17<sup>th</sup>, 2017. The boot camp is a cross-institutional program created by Stanford's Hoover Institution, Center for International Security and Cooperation, and Freeman Spogli Institute for International Studies.

Designed to give select senior congressional staffers a deeper understanding of cybersecurity issues, the boot camp incorporates a broader network of experts from industry and academia to draw upon in the future. You will examine key technical, legal, economic, psychological, and organizational cyber policy challenges, participate in hands on simulations, taught by world renowned faculty, and engage in discussions with Silicon Valley leaders. We have also dedicated time for dialogue and questions that are of particular interest to you.

Confirmed speakers this year include: former Secretary of State Condoleezza Rice, former Ambassador to Russia Michael McFaul, former President of Estonia Toomas Hendrik Ilves, cofounder of Andreessen Horowitz, Marc Andreessen, plus many more from academia, tech, and the policy community. A field trip to Tesla's factory and headquarters is also slated on the agenda.

Stanford University will pay for reasonable travel expenses, including round-trip economy airfare, and ground transportation, business class lodging, and meals. The Boot Camp will not be financed in any part by a registered lobbyist or foreign agent, and will comply with all Congressional ethics rules. To participate in the Congressional Cyber Boot Camp, please reply to Andrew Clark, afclark@stanford.edu, no later than June 30th.

We are very much looking forward to your participation and welcoming you to sunny California this August.

Sincere regards,

Twell 2 tells

Russell C. Wald

Senior Manager for External Affairs
Hoover Institution, Stanford University

# Senate

Last	Frist
Akpa	Stephanie
Arias	Jonathan
Freedman	Brett
Kitchen	Klon
Klein	Julie
Lazarus	Allison
Lips	Dan
McFeely	Tara
Middleton	Bakari
Ravindra	Arjun
Soifer	Halie
Stransky	Michael
Rossi	Nick
Nguyen	Minh
Burwell	Carter



Cyber Boot Camp 2017 Stanford University Palo Alto, CA

Individual Flight Information: Nick Rossi

Outbound flight: August 14, 2017

Flight Number – VX 67
Departure Airport – IAD
Departure Time – 7:20am
Arrival Airport – SFO
Arrival Time – 9:55am

Return Flight: August 27, 2017
Flight Number – Delta 4870/2249
Departure Airport – FAT
Departure Time – 12:30pm
Layover: SLC

Arrival Airport – IAD Arrival Time – 11:27pm

Joining Group: 9:55am on August 14<sup>th</sup>, 2017 Leaving Group: 7:00am on August 17<sup>th</sup>, 2017 PAT ROBERTS, KANSAS BRIAN SCHATZ, HAWAII
JAMES E. RISCH, IDAHO JEANNE SHAHEEN, NEW HAMPSHIRE

DEBORAH SUE MAYER, CHIEF COUNSEL AND STAFF DIRECTOR EMILY GERSHON, CHIEF CLERK

TELEPHONE: (202) 224-2981 FACSIMILE: (202) 224-7416 TDD: (202) 228-3752

# United States Senate

SELECT COMMITTEE ON ETHICS

August 2, 2017

Nicholas A. Rossi Committee on Commerce, Science, and Transportation United States Senate Washington, DC 20510

Dear Mr. Rossi:

This responds to your recent correspondence concerning an invitation you received to travel to the 2017 Stanford Congressional Cyber Boot Camp, in Palo Alto, California on August 14-17, 2017, sponsored by Stanford University's Hoover Institution (Hoover Institution). The Hoover Institution certified to the Select Committee on Ethics (the Committee) that it will pay the necessary expenses related to the travel and that it is neither a lobbyist, nor lobbying firm, nor agent of a foreign principal, and it is not otherwise acting as a representative or agent of a foreign government. However, the Hoover Institution has certified that it is an organization designated under § 501(c)(3) of the Internal Revenue Code<sup>3</sup> that retains or employs a registered lobbyist and that no registered lobbyist will accompany you at any point throughout your trip. 4

Based on information and materials available to the Committee, and assuming the actual travel and travel-related expenses conform to the information and materials you provided, it appears that the proposed payment or reimbursement of necessary expenses for this trip may be accepted under relevant Senate Rules and the Committee's Regulations and Guidelines for Privately-Sponsored Travel, so long as at the time of the payment or reimbursement, Hoover Institution is neither a registered lobbyist nor lobbying firm under the Lobbying Disclosure Act of 1995, nor an agent of a foreign principal under the Foreign Agents Registration Act (and is not otherwise acting as a representative or agent of a foreign government), and provided the travel and all required documents are disclosed to the Secretary of the Senate in accordance with the provisions of Senate Rules 34 and 35.

<sup>&</sup>lt;sup>1</sup> Based on the information you submitted, the Committee understands that, for a personal purpose, you intend to extend your trip in California for ten days after the conclusion of the officially related events. Because your proposed extension is longer than the sponsored trip itself, you must personally pay the full cost of your transportation to and from California, as well as any other additional expenses incurred as a result of extending your trip.

<sup>&</sup>lt;sup>2</sup> The term "necessary expenses" has a specific definition. See Select Committee on Ethics' Regulations and Guidelines for Privately-Sponsored Travel – Glossary of Terms at 8.

<sup>&</sup>lt;sup>3</sup> 26 U.S.C. § 501(c)(3).

<sup>&</sup>lt;sup>4</sup> The term "any point throughout your trip" has a specific definition. See Select Committee on Ethics' Regulations and Guidelines for Privately-Sponsored Travel – Glossary of Terms at 2.

Under Senate Rule 35, Senate staff must receive advance authorization signed by the Member or officer under whose direct supervision the individual works in order to accept payment or reimbursement for necessary expenses related to fact-finding travel. Further, such authorization and expenses must be disclosed to the Secretary of the Senate by filing the completed Employee Pre-Travel Authorization and the Employee Post-Travel Disclosure of Travel Expenses (Form RE-1 and Form RE-2), along with a copy of the Private Sponsor Travel Certification Form, and all relevant attachments (e.g., the private sponsor's invitation and itinerary) within 30 days of the conclusion of Privately-Sponsored Travel.<sup>5</sup>

Finally, Senate Rule 34 requires a reporting individual,<sup>6</sup> on his or her Financial Disclosure Report, to make an annual disclosure of the receipt of payments or reimbursements under Senate Rule 35 from a private sponsor for officially-related travel expenses where, in the aggregate, travel expenses exceed \$390 from that sponsor during a calendar year. However, if a Member, officer, or employee properly reports the receipt of necessary expenses for such travel to the Secretary of the Senate within 30 days of the travel, as discussed above, the travel expenses need not be disclosed a second time on their Financial Disclosure Report.

I hope you find this information helpful. If you have any additional questions, please do not hesitate to contact the Committee.

Sincerely,

Deborah Sue Mayer

Chief Counsel and Staff Director

Enclosure: Travel Checklist

<sup>&</sup>lt;sup>5</sup> Trip extensions for any purpose do not extend this deadline.

<sup>&</sup>lt;sup>6</sup> A reporting individual is someone whose salary equals or exceeds 120% of the basic rate of pay for GS-15 (\$124,406 for CY 2017) or is a political fund designee and is required to file Financial Disclosure Reports.

000000

BRIAN SCHATZ, HAWAII JEANNE SHAHEEN, NEW HAMPSHIRE

Committee's website.

and reasonable.

DEBORAH SUE MAYER, CHIEF COUNSEL AND STAFF DIRECTOR EMILY GERSHON, CHIEF CLERK

TELEPHONE: (202) 224-2581 FACSIMILE: (202) 224-7416 TDD: (202) 228-3752

# United States Senate

SELECT COMMITTEE ON ETHICS

# Employee Privately-Sponsored Travel Checklist

Employees must submit their completed Pre-Travel Authorization Package to the Select Committee on Ethics (the Committee) at least 30 days prior to the travel departure date. Incomplete Pre-Travel Authorization Packages and Packages submitted later than 30 days prior to the travel departure date will not be considered or approved. All of the forms and materials listed below are available as fillable PDFs on the Committee's website at <a href="http://www.ethics.senate.gov">http://www.ethics.senate.gov</a>.

# Pre-Travel Authorization

Review Senate Rules and the Committee's Privately-Sponsored Travel Guidelines on the

☐ Ensure your supervising Senator or Officer (President of the Senate, Secretary of

the Senate, Sergeant at Arms, Secretary for the Majority, Secretary for the

Minority, and Chaplain) has determined the expenses for the trip are necessary

# Prior to Submitting a Pre-Travel Authorization Package to the Committee

Ensure your supervising Senator or Officer has certified the proposed travel is connected to your official duties and will not create any appearance of a public
office being used for private gain.
At Least 30 Days Prior to Trayel: Submit Completed Pre-Travel Authorization Package
File with the Select Committee on Ethics in SH-220
☐ Complete Employee Pre-Travel Authorization Form (Form RE-1)
Ensure this form is typed and that all of the fields are completed.
Ensure your supervising Senator or Officer has signed this form.
Personally sign this form.
☐ Ensure Pre-Travel Authorization Package is complete. A complete Package includes:
☐ Form RE-1
Private sponsor invitation (the formal invitation, letter or e-mail you received
from the private sponsor).
Completed and signed Private Sponsor Travel Certification Form (4 page form
that includes detailed information about the trip).
All attachments to the Private Sponsor Travel Certification Form
Complete and final itinerary
List of Senate invitees
Any other necessary attachments
Retain a copy of your complete Pre-Travel Authorization Package for inclusion in your
required post-travel disclosure.
f A

# 6666666666666

# **EMPLOYEE PRE-TRAVEL AUTHORIZATION**

<u>Pre-Travel Filing Instructions</u>: Complete and submit this form at least 30 days prior to the travel departure date to the <u>Select Committee on Ethics</u> in <u>SH-220</u>. Incomplete and late travel submissions will <u>not</u> be considered or approved. This form <u>must</u> be typed and is available as a fillable PDF on the Committee's website at ethics.senate.gov. Retain a copy of your entire pre-travel submission for your required post-travel disclosure.

Name of Traveler:	Nicholas A. Rossi
Employing Office/Committee:	Committee on Commerce, Science, & Transportation
Private Sponsor(s) (list all): Stanfo	rd University's Hoover Institution
· · · · · · · · · · · · · · · · · · ·	7/2017 (see attached appendix re: anticipated unofficial travel after the trip)
Note: If you plan to extend t	the trip for any reason you <u>must</u> notify the Committee.
Destination(s): Stanford Univers	ity, Palo Alto, CA
Explain how this trip is specifically	connected to the traveler's official or representational duties:
director of the Committee on C	I in major legislation and ongoing oversight regarding cyber security. As staff commerce, Science, & Transportation, traveler continues to oversee legislation, engagement, and hearings on cyber security. Traveler also serves as visor on this issue.
Name of accompanying family men Relationship to Employee: Spou	
I certify that the information contain	ed in this form is true, complete and correct to the best of my knowledge:
7/13/2017	Willer S. Han.
(Date)	(Signature of Employee)
TO BE COMPLETED BY SUPERVISION Secretary for the Majority, Secretary for	ING SENATOR/OFFICER (President of the Senate, Secretary of the Senate, Sergeant at Arms, r the Minority, and Chaplain):
John R. Thune	hereby authorize Nicholas A. Rossi
(Print Senator's/Officer's N	
related expenses for travel to the eve	vision, to accept payment or reimbursement for necessary transportation, lodging, and ent described above. I have determined that this travel is in connection with his or her efficeholder, and will not create the appearance that he or she is using public office for
I have also determined that the attent of the Senate. (signify, "yes" by checking the senate.	dance of the employee's spouse or child is appropriate to assist in the representation $\log box$

(Signature of Supervising Senator/Officer)

# Appendix to Employee Pre-Travel Authorization For Nicholas Rossi (dated July 13, 2017)

The travel dates for this trip are from 08/14/2017 to 08/17/2017. I plan to remain in California for a personal vacation (my in-laws reside in California, and my wife and children will already be in California on vacation) from 08/17/2017 until 08/27/2017. Given that the length of my personal travel will exceed the length of the trip sponsored by Stanford University's Hoover Institution, I will purchase my own airfare to and from California, rather than accepting the airfare offered by the trip sponsor. I will only accept local ground transportation, lodging, and meals that are directly related to the sponsored trip/program. I do not expect to receive any discount for my personal travel costs by participating in the trip and will, in all likelihood, incur additional personal expenses by participating in the sponsored travel that I would not otherwise have incurred (e.g., the cost of renting a car to travel from Palo Alto, CA, to my final vacation destination elsewhere in the state). I have consulted with the Ethics Committee legal staff regarding this plan and received oral guidance that it would be appropriate.



Dear Congressional Staff,

On behalf of Hoover Institution fellows Mike Franc, Herb Lin and Amy Zegart, I would like to formally invite you to participate in Stanford's Congressional Cyber Boot Camp, held in Palo Alto, California on August 14<sup>th</sup> – 17<sup>th</sup>, 2017. The boot camp is a cross-institutional program created by Stanford's Hoover Institution, Center for International Security and Cooperation, and Freeman Spogli Institute for International Studies.

Designed to give select senior congressional staffers a deeper understanding of cybersecurity issues, the boot camp incorporates a broader network of experts from industry and academia to draw upon in the future. You will examine key technical, legal, economic, psychological, and organizational cyber policy challenges, participate in hands on simulations, taught by world renowned faculty, and engage in discussions with Silicon Valley leaders. We have also dedicated time for dialogue and questions that are of particular interest to you.

Confirmed speakers this year include: former Secretary of State Condoleezza Rice, former Ambassador to Russia Michael McFaul, former President of Estonia Toomas Hendrik Ilves, cofounder of Andreessen Horowitz, Marc Andreessen, plus many more from academia, tech, and the policy community. A field trip to Tesla's factory and headquarters is also slated on the agenda.

Stanford University will pay for reasonable travel expenses, including round-trip economy airfare, and ground transportation, business class lodging, and meals. The Boot Camp will not be financed in any part by a registered lobbyist or foreign agent, and will comply with all Congressional ethics rules. To participate in the Congressional Cyber Boot Camp, please reply to Andrew Clark, afclark@stanford.edu, no later than June 30th.

We are very much looking forward to your participation and welcoming you to sunny California this August.

Sincere regards,

Russell C. Wald

Senior Manager for External Affairs
Hoover Institution, Stanford University

# PRIVATE SPONSOR TRAVEL CERTIFICATION FORM

This form must be completed by any private entity offering to provide travel or reimbursement for travel to Senate Members, officers, or employees (Senate Rule 35, clause 2). Each sponsor of a fact-finding trip must sign the completed form. The trip sponsor(s) must provide a copy of the completed form to each invited Senate traveler, who will then forward it to the Ethics Committee with any other required materials. The trip sponsor(s) should NOT submit the form directly to the Ethics Committee. Please consult the accompanying instructions for more detailed definitions and other key information.

The Senate Member, officer, or employee MUST also provide a copy of this form, along with the appropriate travel authorization and reimbursement form, to the Office of Public Records (OPR), Room 232 of the Hart Building, within thirty (30) days after the travel is completed.

Spo	nsor(s) of the trip (please list all sponsors): Stanford University's Hoover Institution
<del></del>	· · · · · · · · · · · · · · · · · · ·
Des	eription of the trip:  An intensive program for congressional staff which consists of three days of
	ninars, simulations, and keynote presentations.
Date	es of travel:
Plac	e of travel: Stanford University, Palo Alto, CA
Nan	ne and title of Senate invitees: See attached list
l ce	rtify that the trip fits one of the following categories:
	(A) The sponsor(s) are not registered lobbyists or agents of a foreign principal and do not retain or employ registered lobbyists or agents of a foreign principal and no lobbyist or agents of a foreign principal will accompany the Member, officer, or employee at any point throughout the trip.  — OR —
	(B) The sponsor or sponsors are not registered lobbyists or agents of a foreign principal, but retain or employ one or more registered lobbyists or agents of a foreign principal and the trip meets the requirements of Senate Rule 35.2(a)(2)(A)(i) or (ii) (see question 9).
	I certify that the trip will not be financed in any part by a registered lobbyist or agent of a foreign principal.
	– AND –
	I certify that the sponsor or sponsors will not accept funds or in-kind contributions earmarked directly or indirectly for the purpose of financing this specific trip from a registered lobbyist or agent of a foreign principal or from a private entity that retains or employs one or more registered lobbyists or agents of a foreign principal.
	rtify that:
X	The trip will not in any part be planned, organized, requested, or arranged by a registered lobbyist or agent of a foreign principal except for <i>de minimis</i> lobbyist involvement.  - AND -
X	The traveler will not be accompanied on the trip by a registered lobbyist or agent of a foreign principal except as provided for by Committee regulations relating to lobbyist accompaniment (see question 9).

9.	USE ONLY IF YOU CHECKED QUESTION 6(B)  I certify that if the sponsor or sponsors retain or employ one or more registered lobby ists or agents of a foreign principal, one of the following scenarios applies:
	<ul> <li>(A) The trip is for attendance or participation in a one-day event (exclusive of travel time and one overnight stay) and no registered lobbyists or agents of a foreign principal will accompany the Member officer, or employee on any segment of the trip.         <ul> <li>OR -</li> </ul> </li> </ul>
	<ul> <li>□ (B) The trip is for attendance or participation in a one-day event (exclusive of travel time and two overnight stays) and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee on any segment of the trip (see questions 6 and 10).</li> <li>- OR -</li> </ul>
	(C) The trip is being sponsored only by an organization or organizations designated under § 501(c)(3) of the Internal Revenue Code of 1986 and no registered lobbyists or agents of a foreign principal will accompany the Member, officer, or employee at any point throughout the trip.
10.	USE ONLY IF YOU CHECKED QUESTION 9(B)  If the trip includes two overnight stays, please explain why the second night is practically required for Senate invitees to participate in the travel:
11.	An itinerary for the trip is attached to this form. I certify that the attached itinerary is a detailed (hourby-hour), complete, and final itinerary for the trip.
12.	Briefly describe the role of each sponsor in organizing and conducting the trip:
	Stanford University's Hoover Institution solely planned all aspects of the trip, including topics to be
	discussed, travel/accommodation logistics, and required paperwork. Hoover employees will also be
	responsible for traveling with congressional staff and managing logistics for the duration of the trip.
13.	Briefly describe the stated mission of each sponsor and how the purpose of the trip relates to that mission:  The Hoover Institution is a research institution that seeks to improve the human condition by advancing
	ideas that promote economic opportunity and prosperity while securing and safeguarding the peace
	through its world renowned scholars, library, and archives, as well as by engaging Congress and its staff.
14.	Briefly describe each sponsor's prior history of sponsoring congressional trips:  This is the third sponsored trip for congressional staff organized by the Hoover
	Institution. The latest of which was in April of 2017 and had a similar format as this trip.

Stanford University's	Hoover Institution regul	arly sponsors policy	panels and roundtab	les for think tar		
scholars, journalists, congressional staff, Executive branch officials, academics, and members of the						
general public.						
Total Expenses for Each Participant:						
	Transportation Expenses	Lodging Expenses	Meal Expenses	Other Expense		
Good Faith estimate  Actual Amounts	\$600 roundtrip airfare; \$200 ground transportation	\$450 total (\$150/night)	\$192 total (\$64/day)	N/A		
participation or b) the congressional particip	ip involves an event that trip involves an event that ation:  rganized specifically for	hat is arranged or org	ganized <i>specifically</i> w	to congression with regard to		
participation or b) the congressional particip	trip involves an event to ation:	hat is arranged or org	ganized <i>specifically</i> w	to congression		
participation or b) the congressional particip  The trip is arranged/or	trip involves an event to ation:	hat is arranged or org	ganized <i>specifically</i> w	to congression		
Participation or b) the congressional particip  The trip is arranged/or  Reason for selecting the selection of the select	trip involves an event to ation:  rganized specifically for	tat is arranged or org	ipation.	vith regard to		
Participation or b) the congressional particip The trip is arranged/or Reason for selecting the light order to have a sign	trip involves an event thation:  rganized specifically for  ne location of the event	congressional partic or trip er senior fellows part	ipation.	vith regard to		
participation or b) the congressional particip The trip is arranged/or Reason for selecting the In order to have a sign the Hoover Institution'	trip involves an event to ation:  rganized specifically for the event of the event	congressional partic or trip er senior fellows part	ipation.	vith regard to		
Participation or b) the congressional particip The trip is arranged/or Reason for selecting the In order to have a sign the Hoover Institution.  Name and location of	trip involves an event thation:  rganized specifically for  ne location of the event history and the second specifical triangles are specifically for the second specifical triangles are second specifical triangles.	congressional partic or trip er senior fellows part Stanford University ca	ipation.	vith regard to		
Participation or b) the congressional particip The trip is arranged/or Reason for selecting the In order to have a sign the Hoover Institution.  Name and location of	trip involves an event to ation:  rganized specifically for the event history of the event history of the second the Seco	congressional partic or trip er senior fellows part Stanford University ca	ipation.	vith regard to		
Participation or b) the congressional particip. The trip is arranged/or Reason for selecting the In order to have a significant the Hoover Institution. Name and location of Schwab Residential Congressions.	trip involves an event to ation:  rganized specifically for the event history of the event history of the second the Seco	congressional partice or trip er senior fellows part callity: anford, CA 94305	ipation.	ve are hosting		

21.	Describe how the daily expenses for lodging, meals, and other expenses provided to trip participants compares to the maximum per diem rates for official Federal Government travel:
	All lodging, meals, and other expenses are within the official federal government travel per diem rate for
	Palo Alto, CA.
22.	Describe the type and class of transportation being provided. Indicate-whether coach, business-class or first class transportation will be provided. If first-class fare is being provided, please explain why first-class travel is necessary:
	Stanford University's Hoover Institution will provide coach-class round-trip airfare between D.C and
	San Fransisco, and round-trip ground transportation between Stanford University from SFO airport.
23.	I represent that the travel expenses that will be paid for or reimbursed to Senate invitees do not include expenditures for recreational activities, alcohol, or entertainment (other than entertainment provided to all attendees as an integral part of the event, as permissible under Senate Rule 35).
24.	List any entertainment that will be provided to, paid for, or reimbursed to Senate invitees and explain why the entertainment is an integral part of the event:
	None .
25.	I hereby certify that the information contained herein is true, complete and correct. (You must include the completed signature block below for each travel sponsor.):  Signature of Travel Sponsor:  M. M. G. Hare
	Name and Title: Michael G. Franc, Director of Washington, DC Programs
	Name of Organization: Hoover Institution
	Address: 1399 New York Ave NW, Suite 500, Washington, DC 20005
	Telephone Number: (202) 760-3200
	Fax Number: (202) 760-3191
	E-mail Address:mfranc@stanford.edu

Last Name	First Name	<u>Title</u>	Committee/Office	Chamber	Partv	Gende
Akpa	Stephanie	Policy Counsel	Senator Warren	Senate	D	F
Arias	Jonathan	MLA	Senator Rubio	Senate	R	М
Batch	Brandon	Senior LA	Rep. McCaul	House	R	М
Bergin	Moira	Staff Director	Homeland Subcommittee	House	D	F
<del></del>		Democratic Staff				
Bergreen	Tim	Director	HPSCI	House	D	М
			Committee on Small			
Burchfield	James	PSM	Business	House	R	M
		Deputy Chief	Subcommittee on			
Burwell	Carter	Counsel	Constitution (Judiciary)	Senate	R	М
Carroll	Melika	Policy Advisor	Senator Schatz	Senate	D,	F
<u> </u>		National Security				
Dressler	Jeff	Advisor	Speaker Ryan	House	R	М
Everett	Jason	Chief Counsel	Judiciary Sub	House	D	М
Freedman	Brett	Counsel	SSCI	Senate	D	М
		National Security				
Geer	Harlan	Advisor	Senator Hassan	Senate	D	М
		Chief Oversight				
Hiller	Aaron	Counsel	Committee on Judiciary	House	D	М
		Senior Policy				
Jacobson	Corey	Advisor	Rep. Ted Lieu	House	D	М
			Judiciary Sub (Courts, IP,		·	
Keeley	Joe	Chief Counsel	Internet)	House	R	М
		National Security				
Khrestin	lgor	Advisor	Senator Garner	Senate	R	M
King	Elizabeth	Staff Director	SASC	Senate	D	F
•		National Security				
Kitchen	Klon	Advisor	Sasse	Senate	R	М
Klein	Julie	PSM	HSGAC	Senate	D	F
Lazarus	Allison	PSM	SASC	Senate	R	F
Lips	Dan	PSM	HSGAC	Senate	R	М
		Democratic Staff	Commerce, Science,			
Lipsky	Kim	Director	Transportation	Senate	D	F
			Oversight and Gov			
Lynch	Tim	Senior Counsel	Reform	House	D	М
			Subcommittee on Cyber			
Mat <u>thews</u>	Madeline	PSM	(Homeland)	House	R	F
McElivein	Elizabeth	PSM	Judiciary Committee	House	D	F
McFeely	Tara	PSM	SSCI	Senate	R	F

Middleton	Bakari	Counsel	Booker	Senate	D	M
Nguyen	Minh	General Counsel	Senator McCain	Senate	R	F
Park ·	Chan	General Counsel	Committee on Judiciary	Senate	D	M
		Deputy Chief of				
Po	Rosa	Staff	Senator Klobuchar	Senate	D	F
Ravindra	Arjun	PSM	SSCI	Senate	R	М
			Commerce, Science,			
Rossi	Nick	Staff Director	Transportation	Senate	R	М
Smith	Angel	PSM	HPSCI	House	R	F
		National Security				
Soifer	Halie	Advisor	Senator Harris	Senate	D	F
Steward	Lindsay	PSM	Subcommittee Oversight	House	R	F
Stock	Troy	Senior Counsel	Oversight	House	R	М
Tuttle	Chris	Staff Director	Foreign Relations	Senate	R	М



Cyber Boot Camp 2017 Stanford University Palo Alto, CA

# Group Flight Information:

Outbound flight: August 14, 2017
Flight Number – VX 67
Departure Airport – IAD
Departure Time – 7:20am
Arrival Airport – SFO
Arrival Time – 9:55am

Return Flight: August 17, 2017
Flight Number – VX 1
Departure Airport – SFO
Departure Time – 8:00am
Arrival Airport – DCA
Arrival Time – 4:05pm



# SYLLABUS

# **FACULTY CO-CHAIRS**

# Dr. Amy Zegart

Co-Director, Center for International Security and Cooperation (CISAC)
Davies Family Senior Fellow, Hoover Institution
Senior Fellow, Freeman Spogli Institute for International Studies (FSI)
Professor of Political Science (by courtesy), Stanford University

### Dr. Herb Lin

Senior Research Scholar for Cyber Policy and Security, Center for International Security and Cooperation (CISAC)

Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution
Chief Scientist Emeritus, Computer Science and Telecommunications Board, National
Academies

### **COURSE DESCRIPTION**

Modern nations are increasingly dependent on information and information technology for societal functions. Thus, ensuring the security of information and information technology — cybersecurity — against a broad spectrum of hackers, criminals, terrorists, and state actors is a critical task for the nation. Cybersecurity challenges are evolving at a rapid pace, and the cyber threat the nation faces today will be different from the one it faces tomorrow.

Cybersecurity is not solely a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Improving cybersecurity is a multi-faceted enterprise that requires drawing on knowledge from computer science, economics, law, political science, psychology, and a host of other disciplines. Therefore, this Boot Camp draws upon the expertise of cyber scholars in academia as well as senior business and security professionals in Silicon Valley to provide perspectives on the many dimensions of this dynamic issue.

This Boot Camp will integrate multiple perspectives and disciplines to provide an understanding of the fundamentals of cybersecurity, the nature of cybersecurity threats, various approaches to

addressing these threats, and the use of offensive cyber capabilities to advance national interests. The Stanford Cyber Boot Camp endeavors to give congressional staffers a conceptual framework to understand the threat environment of today and how it might evolve so that they are better able to anticipate and manage the problems of tomorrow.

# Day 1 (Monday, August 14): Cyber Attacks and Responses

12:00 p.m. - 1:00 p.m.: Lunch & Keynote Address

# FRAMING THE CYBERSECURITY PROBLEM

# **Faculty:**

Sean Kanuck, Former National Intelligence Officer for Cyber Issues, Office of the Director of National Intelligence; CISAC affiliate

This session will overview the scope of the program (what we cover, what we don't, and why) and set the analytic stage for how we approach the rest of the course.

**Scope**: The security implications and challenges of the nation's use of information technology. The course does not address topics such as consumer security, although many concepts covered are relevant.

Framing Theme #1: Cybersecurity has different meanings and poses different challenges to different stakeholders. Approaching the problem posed requires understanding the perspectives of various actors, their interests, incentives, and organizational demands. Boot Camp sessions are designed to allow staffers to better understand the perspectives of different stakeholders and key players, including attackers and corporate executives.

**Framing Theme #2**: The non-technical dimensions of cybersecurity (politics, organizational dynamics, economics, and psychology) are often far more important and less understood than the technical aspects. The Boot Camp pays explicit attention to these non-technical dimensions and how they intersect with technical challenges.

Framing Theme #3: On the technical side, the course focuses on the underlying foundational principles of computing and communications technology (collectively, information technology) that drive the evolution of architectures, technologies, and vulnerabilities.

Framing Theme #4: The Boot Camp explains the inherent dominance of offense over defense in cybersecurity and how this fact relates to the "cybersecurity problem."

1:00 p.m. - 2:00 p.m.: Session 1

### THINKING LIKE AN ATTACKER

### Faculty:

**Peiter Zatko,** Cyber Independent Testing Lab **Dr. Herb Lin (Discussant),** Senior Research Scholar, CISAC; Hank J. Holland
Fellow, Hoover Institution

Effectively combating any adversary requires understanding the ways in which that adversary thinks. Cybersecurity adversaries — from state agents seeking to disable military systems to hacktivists seeking to make a political point — share a security mindset: a predilection for examining the ways in which the security of a system can be circumvented or penetrated. Whereas good engineering is about how a system can be made to work, the security mindset involves thinking about how some aspect of a system can be made to fail. Understanding this mindset is the first step towards designing sound cybersecurity solutions.

<u>Assignment:</u> While in transit to the course location in Palo Alto, conduct a thought experiment for bringing an item prohibited by TSA regulations onto the airplane.

<u>Learning Objectives:</u> Why defense is more difficult than offense and what makes ongoing offense-defense competition inevitable.

2:30 p.m. – 3:30 p.m.: Session 2

THREATS TO CYBERSECURITY

# Faculty:

Carey Nachenberg, Google X; Adjunct Assistant Professor of Computer Science, UCLA

Cybersecurity compromises can take a variety of forms and occur for a variety of reasons. Session 2 examines these compromises and the vulnerabilities in information technology that allow them to happen, again reprising the theme of offensive dominance. This session will include a number of forensic case studies that illuminate the attack spectrum, key challenges, and trends.

<u>Learning Objectives</u>: Security-relevant principles of information technology; types of compromise; the inherent vulnerabilities of information technology; the hidden complexity of cyberspace; anatomy of security compromises; and the spectrum of threats to cybersecurity.

# 3:45 p.m. - 4:15 p.m.: Keynote Remarks

### THE VIEW FROM EUROPE

# Faculty:

**Toomas Hendrik Ilves,** Former President of Estonia; Distinguished Visiting Fellow at CISAC, Hoover, and FSI

# 4:30 p.m. - 5:30 p.m.: Dinner & Session 3

## OFFENSIVE DIMENSIONS OF CYBERSECURITY

# Faculty:

Jason Healey, Senior Research Scholar, Columbia University's School for International and Public Affairs

**Dr. Herb Lin,** Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution

Offensive activities — including those conducted for espionage and attack purposes —serve a variety of national goals. These goals include, but are not limited to, cyber defense. This discussion will summarize the required strategy, intelligence, and policy necessary for offensive cybersecurity.

<u>Learning Objectives</u>: The role of offensive operations in cyberspace for improving the nation's cybersecurity posture and for other purposes; the differences between attacks and exploitations and the importance of these differences; the scope and nature of U.S. command and control of offensive operations in cyberspace.

6:00 p.m. - 8:30 p.m.: Session 4

# SIMULATION: RESPONDING TO A CYBER CRISIS

# Faculty:

Michael McNerney, Cofounder and CEO of Efflux Systems; CISAC Affiliate Raj Shah, Managing Partner, Defense Innovation Unit Experimental (DIUx) Joe Sullivan, Chief Security Officer, Uber

**Ruby Zefo,** Vice President of the Law & Policy Group and Chief Privacy & Security Counsel, Intel Corporation

**Dr. Amy Zegart,** Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

In this exercise, congressional staffers assume the roles of business executives at a large tech company called Frizzle that has just discovered a major cyber breach. Early forensics indicate that a Frizzle employee opened a malicious PDF file containing a zero-day exploit. This vulnerability enabled the attackers to gain access to F-Net, the company's social networking platform, as well as the Frizzle email user accounts of Chechen activists and sympathizers. In addition, the malicious file may have spread through victims' emails to the Credit Luxe bank in Luxembourg, which processes more than two thirds of Frizzle's user payments. Frizzle's engineering/cybersecurity team, which is one of the best in the world, believes the attack came from Eastern Europe, though much remains unclear.

The CEO has called an emergency meeting of the Board of Directors to formulate a broad-based response to the cyber breach and has asked each of Frizzle's core teams – Engineering / Cybersecurity, Business Strategy, Legal, Public Policy, and Marketing / Communications – to develop and present actionable recommendations to the Board.

The Board of Directors is played by leading Silicon Valley security specialists, lawyers, and entrepreneurs with extensive experience in cybersecurity and business. Board Members attend team breakout sessions and in the "full board meeting" question and discuss each team's recommendations. The simulation concludes with a debrief session where staffers reflect on the simulation and Board Members share insights from their actual experiences confronting cyber challenges.

Learning Objectives: To walk in the shoes of business leaders confronting the early hours and critical decisions of a cyber crisis. Who exactly is hurt or could be hurt by the breach? How could the breach impact Frizzle's business in different markets and its brand reputation? Who are the key stakeholders and how might they react? What actions should Frizzle take and what are the tradeoffs? Should the company "hack back" or publicize the breach to its users, its European bank, its competitors? Work with U.S. government agencies? How do Frizzle's mission and corporate culture guide its response? These are some of the questions staffers will consider.

# Day 2 (Tuesday, August 15): Deep Dive: Technical & Nontechnical Aspects of Cyber

8:30 a.m. - 10:00 a.m.: Breakfast and Keynote Conversation

**KEYNOTE** 

Conversation with Dr. Condoleezza Rice and Marc Andreessen

# Faculty:

**Dr. Condoleezza Rice,** Thomas and Barbara Stephenson Senior Fellow, Hoover Institution; Denning Professor, Stanford Graduate School of Business; former U.S. Secretary of State and National Security Advisor

Marc Andreessen, Cofounder and General Partner of Andreessen Horowitz

10:15 a.m. - 11:15 a.m.: Session 5

# **FUNDAMENTAL PRINCIPLES OF CYBERSECURITY**

### Faculty:

Dr. Irving Lachow, Portfolio Manager, International Cyber, MITRE; Visiting Fellow, Hoover Institution; Affiliate, CISAC

**Dr. John Villasenor,** Professor of Electrical Engineering, Public Affairs, and Management, UCLA; Vice Chair, World Economic Forum's Global Agenda Council on the Intellectual Property System; Visiting Fellow, Hoover Institution; Affiliate, CISAC

Although cybersecurity can be a deeply technical subject, especially in how cybersecurity solutions are implemented, a few fundamental principles underlie most solutions. This session takes a deep dive into the fundamental principles of improving cybersecurity and how they fit together. These include reducing reliance on information technology, detecting cybersecurity compromises, and blocking and limiting the impact of compromise. Additional topics include authentication, access control, forensics, recovery, containment, resilience, and active defense.

<u>Learning Objectives</u>: The value of these fundamental principles of cybersecurity and how they can be used collectively to improve security.

# 11:45 a.m. - 12:45 p.m.: Lunch & Session 6

# **ECONOMIC, PSYCHOLOGICAL & ORGANIZATIONAL DIMENSIONS OF CYBERSECURITY**

# Faculty:

**Dr. Dave Clark,** Senior Research Scientist at the MIT Computer Science and Artificial Intelligence Laboratory

**Dr. Tyler Moore,** Tandy Assistant Professor of Cyber Security and Information Assurance, University of Tulsa

Known cybersecurity measures are often fully adopted due to a variety of economic, psychological, and organizational factors. These factors are non-technical in nature and often underappreciated by technical and policy communities. Economics describe the incentives that apply to cyber defenders and adversaries, including the nature of cybersecurity market failures and the ability to handle collective action problems. Psychology addresses the deception primary to cybersecurity attacks and the uncertainty of most decision-making in response. An organizational perspective addresses the structural necessities and importance of organizational culture to cybersecurity. This session examines how these factors often discourage the adoption of sound security practices.

<u>Learning Objectives</u>: The importance of economic, organizational, and psychological factors of cybersecurity and why they are often overlooked in efforts to improve cybersecurity; how government action might help to address non-technical factors that diminish the nation's cybersecurity posture.

1:30 p.m. - 2:30 p.m.: Session 7

# DOMESTIC LAW AND INTERNATIONAL LEGAL DIMENSIONS OF CYBER SECURITY

### Faculty:

Prof. Matthew Waxman, Liviu Librescu Professor of Law, Faculty Chair Roger Hertog Program on Law and National Security, Columbia University
Prof. Robert Chesney, Associate Dean and Charles I. Francis Professor,
University of Texas School of Law; Director, Robert S. Strauss Center for International Security and Law

Technological change has far outpaced changes in law and will almost certainly continue to do so in the future. This lag consequentially challenges Congress to craft legislation appropriate for future technology. Furthermore, nations have cooperative and competitive (and sometimes

adversarial) interests that play out in cyberspace. Internet communication does not inherently respect national borders, giving an international dimension to every cybersecurity challenge.

<u>Learning Objectives</u>: For domestic law, the implicit technological assumptions of existing cybersecurity laws; what problems arise in applying existing law to technological circumstances not contemplated at the time of initial passage.

For international dimensions, various legal regimes of potential relevance, including the law of war, human rights law, trade and intellectual property law; proposals for Internet governance; and different non-governmental organizations that affect the design and operation of the Internet.

2:30 p.m. - 3:00 p.m.

**DEBRIEF** from previous day

# Faculty:

Dr. Herb Lin, Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution

Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

5:30 p.m. – 8:30 p.m.; Reception & Dinner

**KEYNOTE** 

Conversation between Dr. Michael McFaul and Joel Peterson

~°

# **Faculty:**

Dr. Michael McFaul, Director and Senior Fellow, FSI; Peter and Helen Bing Senior Fellow, Hoover Institution, Professor of Political Science, Stanford University; former U.S. Ambassador to the Russian Federation Joel Peterson, Chairman, Jet Blue Airways; Robert L. Joss Adjunct Professor of Management, Stanford Graduate School of Business; Chairman, Hoover Institution Board of Overseers

# Day 3 (Wednesday, August 16): Civil Liberties, Corporate Interests, and Security

7:45 a.m. - 8:30 a.m.: Breakfast

**DEBRIEF from previous day** 

# Faculty:

**Dr. Herb Lin,** Senior Research Scholar, CISAC; Hank J. Holland Fellow, Hoover Institution

Dr. Amy Zegart, Co-Director, CISAC; Davies Family Senior Fellow, Hoover Institution; Senior Fellow, FSI

8:30 a.m. - 9:30 a.m.: Session 8

CYBERSECURITY AND CIVIL LIBERTIES

# Faculty:

Anne Neuberger, National Security Agency
Jennifer Granick, Director of Civil Liberties, Stanford Center for Internet and
Society; Affiliate, CISAC; Former Civil Liberties Director, Electronic Frontier
Foundation

Measures intended to support cybersecurity can also threaten certain civil liberties. What cybersecurity means depends in part on whose security is at risk. For some, a threat to civil liberties resulting from greater use of information technology might be interpreted as a cybersecurity threat. Session 8 focuses on this push and pull between security and civil liberties in cyberspace.

<u>Learning Objectives</u>: Different perspectives at the nexus of civil liberties and cybersecurity; how, when, and to what extent, preservation of civil liberties and cybersecurity trade off against one another. Topics to be discussed include privacy, anonymity, and free speech.

9:30 a.m. - 10:30 a.m.: Session 9

### **CORPORATE PERSPECTIVES ON CYBERSECURITY**

## Faculty:

Dr. Sameer Bhalotra (Chair), Co-Founder and CEO, StackRox; Senior Associate of the Strategic Technologies Program, CSIS; Affiliate, CISAC; former Senior Director for Cybersecurity, National Security Council Rick Howard, Chief Security Officer at Palo Alto Networks

Matt Miller, Partner at Sequoia Capital

Market forces have a critical role in enhancing or weakening cybersecurity. Session 9 examines how such forces play out at the level of the individual firm and incorporate the views and concerns of the business community. Silicon Valley senior executives and engineers will give their "cyberground truths" about the security problems facing the private sector.

<u>Learning Objectives</u>: Various private sector perspectives from technology firms that support innovative efforts for providing IT-based products and services with attention to cybersecurity.

11:00 p.m. – 11:45 p.m.: Session 10

WHITE HOUSE PERSPECTIVES

# **Faculty:**

Andy Grotto, CISAC Perry Fellow; Hoover Research Fellow; Affiliate, CISAC; Former Senior Director for Cybersecurity Policy, National Security Council

12:00 p.m. - 1:30 p.m.: Lunch Keynote

DRIVERLESS CARS & PLANE HACKING: SECURITY VULNERABLITIES, CAUSES, AND CHALLENGES

### Faculty:

Dr. Stefan Savage, Professor of Computer Science and Engineering, UCSD; Director, Center for Network Systems (CNS); Co-Director, Center for Evidence-based Security Research (CESR)

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced

a range of new potential risks. In 2010, University of California, San Diego and the University of Washington demonstrated the ability to remotely control a popular passenger vehicle with no prior physical access. Recent demonstrations have validated that similar issues exist in other vehicles as well.

<u>Learning Objectives</u>: The nature of automotive security vulnerabilities, the underlying causes, and the challenges (both technical and non-technical) in securing the automotive platform.

2:30 p.m. – 4:30 p.m.

**TESLA FACTORY VISIT** 

45500 Fremont Blvd, Fremont, CA 94538

5:30 p.m. – 8:30 p.m.

**DINNER & FEEDBACK SESSION** 

Coupa Café – Stanford Golf Course 198 Junipero Serra Blvd, Stanford, CA, 94305